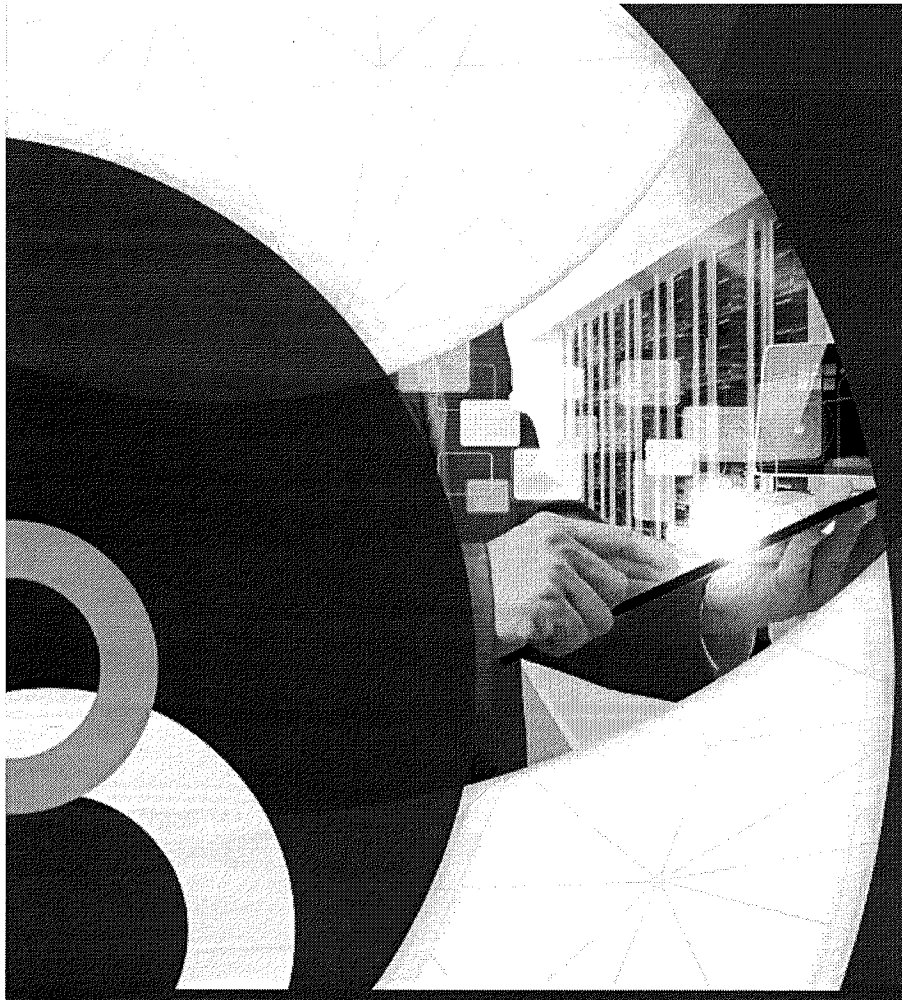


Classification: UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Smart Cities Challenge Webinar

Cyber Security

Communications Security Establishment | Centre de la sécurité des télécommunications

CERRID [illegible]

Canada

Introduction

- Why should you care about Cyber Security?
- What is it?
- Why does Privacy matter and how does it relate to Cyber Security?
- Where do I start with Cyber Security?
- What should you do when your Cyber Security is compromised?

Why should you care about Cyber Security?

- Protect yourself from:
  - Project / program failure
  - Embarrassment & reputational damage
  - Legal repercussions for Privacy breaches
    - Federal: PIPEDA, Office of the Privacy Commissioner (OPC)
    - Provincial Privacy Legislation, Privacy Commissioners

What is Cyber Security?

Definition of *cybersecurity*: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. (Merriam-Webster Dictionary)

- The set of technical and operational measures owners must deploy to ensure that their systems are adequately protected from hostile or malicious actors and from accidents/errors.
- "Adequate protection" depends on what is being protected…

Information as an Asset

- Assets are traditionally seen as physical things. Information is also an asset with unique characteristics:
  - Can be "stolen" yet remain in place
  - Can be modified or corrupted on a large scale with little indication
  - Can be held hostage while still in your possession
  - Unlike physical assets, IT systems can typically be accessed locally or remotely, so your information can both be compromised by an insider threat or without the perpetrator even being on the same continent

Information Security - Types of Injury

- Confidentiality
  - How sensitive is the data?
  - Is there any Personally Identifiable Information (PII) or Personal Health Information (PHI)?
- Integrity
  - What are the consequences of data errors, manipulation, or corruption?
- Availability
  - How long can you go without your data?
  - What are the consequences of permanently losing your data?
- Privacy
  - What are the legal requirements for consent, usage, and disposal?

Threat Actors - Deliberate

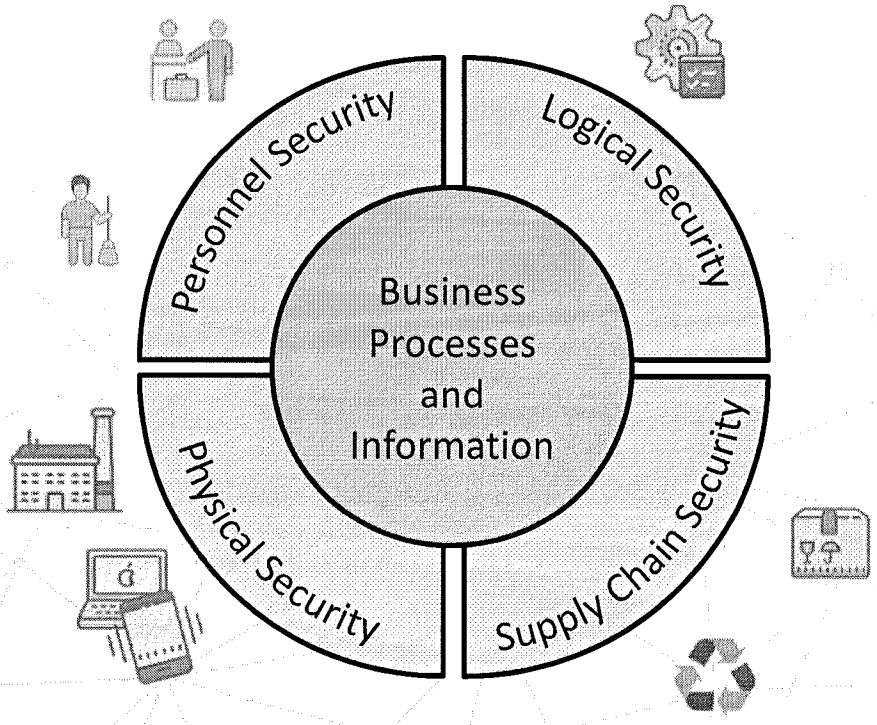
- Who cares about your data (besides you)?
  - Organized Crime
    - ID theft, financial theft, ransomware
  - Nation States
    - Espionage, IP theft, commercial advantage
  - Commercial Espionage
    - Commercial advantage, IP theft, embarrassment & loss of trust
  - Hackers
    - Bragging rights, social activism, grudge, financial gain

Threat Actors – Accidental or Natural

While not necessarily directed at you, your IT still needs to deal with Accidental or Natural threats.

- Accidental
  - Power failures, back-hoes cutting power/communications cables, equipment failures, misconfigurations…
- Natural
  - Tornadoes, floods, fires, ice storms…

Cyber Security - Threat Surfaces



Limiting Threat Surfaces

- Personnel Security
  - Personnel vetting, trustworthiness to counter the "insider threat"
- Physical Security
  - Locked doors, security guards and services, fire prevention and barred windows
- Logical Security
  - Technical security measures in place to protect IT systems
- Supply Chain Security
  - Ensure that products and services are procured from trustworthy suppliers
  - Talk to your suppliers/partners about their supply chain processes

Privacy and Cyber Security

The ultimate authorities on privacy in Canada are the Office of the Privacy Commissioner and their provincial counterparts. Canadian privacy laws such as:

- The Personal Information Protection and Electronic Documents Act (PIPEDA)
- The Privacy Act
- Provincial privacy laws

… seek to establish reasonable standards for the collection, protection, use and destruction of private information.

Privacy and Cyber Security

PIPEDA defines 10 Privacy Principles. In terms of Cyber Security, we are mostly interested in 7 – Safeguards:

PIPEDA Privacy Principles	
1 - Accountability	6 - Accuracy
2 - Identifying Purposes	7 - Safeguards
3 - Consent	8 - Openness
4 - Limiting Collection	9 - Individual Access
5 - Limiting Use, Disclosure, and Retention	10 - Challenging Compliance

PIPEDA Fair Information Principle 7 – Safeguards

- Your responsibilities under PIPEDA:
  - Comply with all 10 of the principles of Schedule 1.
  - Protect personal information against loss or theft.
  - Safeguard the information from unauthorized access, disclosure, copying, use or modification.
  - Protect personal information regardless of the format in which it is held.

In this sense, your Cyber Security mechanisms will provide the tools by which you will meet these safeguarding responsibilities.

Provincial Privacy Requirements

- Provincial PII/PHI Statutes
  - British Columbia's *Personal Information Protection Act*.
  - Alberta's *Personal Information Protection Act*
  - Québec's An Act Respecting the Protection of Personal Information in the Private Sector.
  - Ontario's *Personal Health Information Protection Act*, with respect to health information custodians.
  - New Brunswick's *Personal Health Information Privacy and Access Act*, with respect to personal health information custodians.
  - Nova Scotia's *Personal Health Information Act*, with respect to health information custodians.
  - Newfoundland and Labrador's *Personal Health Information Act*, with respect to health information custodians.
- PIPIDA applies in the absence of Provincial Legislation

Where do I start with Cyber Security?

IT systems can vary widely in both capability and injury level, but generally Cyber Security activities should start with:

- Identifying your data assets
- Identifying potential injuries to them
- Assessing threats and vulnerabilities to determine appropriate Cyber Security measures
- Calculating exposure (Residual Risk)

There are formalized mechanisms for this such as the CSE and RCMP's Harmonized Threat and Risk Assessment process.

Risk Assessments – How exposed are you?

- Threat-Risk Assessment (TRA)
  - Assesses (realistic) threats and vulnerabilities, calculates exposure (Residual Risk)
  - Typically contracted out to a Security Practitioner
  - A TRA often feeds into a PIA
- Privacy Impact Assessment (PIA) Mandated for Federal Departments
  - Privacy Impact Assessments (PIAs) are used to identify the potential privacy risks of new or redesigned federal government programs or services. They also help eliminate or reduce those risks to an acceptable level.

Privacy Impact Assessment (PIA)

- A PIA is designed to accomplish three goals:
  - Ensure conformance with applicable legal, regulatory, and policy requirements for privacy
  - Determine the risks and effects of collecting PII/PHI
  - Evaluate protections and alternative processes to mitigate potential privacy risks

What should you do when your Cyber Security is compromised?

- Despite your best efforts to secure your data, you have to be prepared to act if it is compromised.
  - Do you and your employees have clearly defined roles in case of a compromise?
  - Do you have any means to monitor your systems to detect a compromise?
  - Do you have a clear set of operational procedures to follow in case of a compromise, including points of contact?
  - Do you have a disaster recovery plan in place?

What Sort of Bad Stuff is Out There?

- DDOS
  - Canadian Government Websites
- Ransomware (Wannacry)
  - Midland & Wasaga Beach ON
- Intellectual Property Theft/Competitive Advantage
  - NRC/Potash Corporation
- Private Health Data Theft:
  - CarePartners privacy breach – Thousands of patient records stolen
- Insider Threat by Disgruntled Employees
  - San Francisco

Prevention & Detection

- Use supported software & apply security patches
- Harden your system
  - Center for Internet Security (CIS) baseline
  - Microsoft Security Baseline
  - PCI-DSS
  - NIST Cyber Security Framework Small and Medium Business Resources
- Monitor your system
  - SIEM log processor
  - Antivirus

Prevention & Detection (Continued...)

- Leverage commercial providers if you lack in-house resources
- Engage a Security Professional
- For larger systems, design and assess your system against recognized standards:
  - ISO 27001, NIST 800-53, ITSG-33, NIST Cyber Security Framework

Considerations for Large Data Sets

Many Smart Cities projects are grappling with how to handle large data sets, often containing Personal Information. Some things to consider:

- If you are storing the data yourself, physical and logical access control, backup, encryption and scalability will need to be addressed.
- Managed service providers (including cloud service providers) can address many of these issues for you, but pay attention to privacy laws with respect to data residency as well as cost.
- Data anonymization, the process of removing identity data to allow sharing of large data sets, is a complex and difficult process. Seek out expertize if this is outside of your skill set.

Considerations for Large Data Sets (Continued…)

- Aggregation – is the collection more than the sum of the parts?
- PII – raises the stakes
- Storage – Who has access? Where is it stored?
- Backup – it is being done, right? Who and where?
- Sharing – do you need to share your data? With who? Why?
- Authorized Access – do you know who's accessing your data?
- Citizen Access for PII/PHI – by law: view, modify, correct, remove
- Consider leveraging Commercial Services (such as Cloud)

Incident Response

- Have a plan, and test it periodically
- Isolate the system to contain the breach
- Decide how to proceed – remediate or prosecute?
- Contact CCCS/RCMP
- Commercial IR services
- What needs to be fixed to prevent a reoccurrence?
- Where's your backup?

Incident Response and Recent Changes to PIPEDA

As of November 1, 2018, organizations subject to The Personal Information Protection and Electronic Documents Act (PIPEDA) will be required to:

- Report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals;
- Notify affected individuals about those breaches, and;
- Keep records of all breaches.

Wrap Up

- Cyber Security is a constantly evolving landscape, putting together a solid cyber security foundation is essential
- Consider the legal, reputational, program implications for Cyber Security failures
- Consider engaging professional help in areas outside of your expertise
- The Internet is a very hostile place, so make plans to secure your systems from day one, but expect breach and be prepared to respond and recover

Questions?

Contacts

- Canadian Centre for Cyber Security:
  - Email: contact@cyber.gc.ca
    Toll Free: 1-833-CYBER-88 (1-833-292-3788)
    Local: 613-949-7048
- There are many Cyber Security resources available at:
  - https://cyber.gc.ca/en/

Helpful Links

- PIPEDA Principles
  - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/
- Harmonized Threat and Risk Assessment:
  - https://www.cse-cst.gc.ca/en/system/files/pdf_documents/tra-emr-1-e.pdf
- Incident Examples:
  - https://www.thestar.com/news/canada/2015/06/17/canadian-government-websites-hit-with-massive-outage.html
  - https://barrie.ctvnews.ca/first-wasaga-beach-now-midland-hit-by-cyber-attack-1.4079698
  - https://business.financialpost.com/technology/canada-must-ramp-up-cyber-security-in-wake-of-china-led-attacks-experts-say
  - https://www.carepartners.ca/Privacy-Breach-Update.htm
  - https://www.wired.com/2008/07/insider-tech-at/
- Cyber Security Guidance for Smaller Organizations:
  - https://www.nist.gov/cyberframework/small-and-medium-business-resources